Benoît Thieulin : « Nous pouvons basculer dans une société de surveillance totale »

PAR JÉRÔME HOURDEAUX ET LOUISE FESSARD
ARTICLE PUBLIÉ LE MERCREDI 11 DÉCEMBRE 2013

Le Conseil national du numérique s'est auto-saisi du fameux article 13 de la Loi de programmation militaire. Son président appelle à un *« vrai débat »* sur les questions de surveillance dans l'optique d'une grande loi annoncée pour 2014.

Au lendemain du vote définitif du projet de loi de programmation militaire, Benoît Thieulin, président du Conseil national du numérique (CNNum) qui s'est saisi du dossier, revient sur l'adoption de ce texte, censé encadrer les écoutes administratives mais qui a déclenché un véritable tollé parmi les défenseurs des libertés numériques, ainsi que chez les acteurs économiques du secteur. Il appelle à un *« vrai débat »* sur les questions de surveillance et annonce le lancement d'une *« concertation »* visant à *« nourrir »* la *« future grande loi que Fleur Pellerin* ***a annoncée pour 2014*** *»*.

Lors de son institution, le CNNum était censé « irriguer » toutes les décisions du gouvernement dans le domaine du numérique. Or, sur ce texte et notamment sur l'article 13 qui traite directement des réseaux, vous avez été obligés de vous auto-saisir. Cela ne pose-t-il pas un problème de méthode ?

Benoît Thieulin.- Au-delà de sa capacité d'auto-saisine (qui ne peut être la règle, mais l'exception), le CNNum est saisi par n'importe quel membre du gouvernement. En effet, cela n'a pas été le cas pour la loi de programmation militaire (LPM). Qui plus est, l'article 13, comme vous le savez, est d'origine parlementaire. C'est aussi ce qui explique que la Cnil n'ait pas été saisie de cet article, mais simplement auditionnée. Ce qu'elle a déploré.

Il y a, dans ce texte, des tensions contradictoires ce qui, vu le sujet, n'est pas anormal : lorsqu'on touche à des sujets dont les enjeux sont aussi stratégiques pour un pays que fondamentaux pour le droit des individus, il faut nécessairement viser à un équilibre entre protection individuelle (protéger les libertés de nos concitoyens) et protection globale (défendre les intérêts économiques et scientifiques de notre pays, mais aussi sa sécurité, sa souveraineté).

Ainsi, la LPM tente vraisemblablement de régulariser un certain nombre de pratiques avérées par les services de renseignements français (que Mediapart a contribué à révéler). Franchement, il est difficile de ne pas s'en réjouir, pas par simple principe, mais parce que c'est la seule manière pour la Cnil de pouvoir intervenir ; sans quoi elle doit faire la preuve de ces pratiques, autant dire que c'est peu probable… sauf à protéger davantage les lanceurs d'alerte. On y reviendra…

Ensuite, on peut noter une louable volonté de rattrapage technologique. Nous sommes dans une guerre économique informationnelle : la compétitivité de notre pays, ça n'est pas que sa fiscalité ! C'est aussi et surtout sa capacité d'innovation, la maîtrise de ses datas de masse, etc. On ne peut d'un côté gémir sur la perte de compétitivité du pays, être les premiers à faire les valises pour Londres (avant c'était Koblenz…) et de l'autre déplorer que ce rattrapage ait lieu au sein de nos armées : n'oublions pas le rôle joué dans la révolution numérique que nous vivons par les gigantesques investissement réalisés, voilà 50 ans, par le Pentagone. La France n'a d'ailleurs pas été en reste dans ce mouvement. Sauf récemment.

Enfin, et il faut le souligner, ce texte ajoute des procédures et fusionne des régimes éclatés entre plusieurs lois. On ne peut pas dire qu'il soit dépourvu d'efforts de vouloir encadrer davantage certaines pratiques.

Sauf que les enjeux juridiques entremêlés de dimensions très technologiques rendent très difficile la compréhension de l'impact réel de cet article 13. Ce n'est pas que moi qui le dis :

– l'article du *Canard enchaîné* de la semaine dernière, le remarquable dossier analysé par Arrêt sur images, le soulignent ;

– même, Jean-Marc Manach qu'on ne peut guère soupçonner de sympathie orwellienne reconnaît avec une très belle honnêteté intellectuelle sur son blog qu'il n'arrive toujours pas bien à comprendre si cet

article 13 va permettre, comme l'affirme Jean-Jacques Urvoas, de *«mieux encadrer les services »*, de *«faire bénéficier nos concitoyens de la meilleure garantie de leurs libertés fondamentales au moment de créer des capacités intrusives »*;

– cette étude enfin que je viens de découvrir (grâce à Manach) (**http://ifrei.org/tiki-download_file.php?fileId=59**) pointe également : *«La formulation du L 246-1 ne semble pas intelligible, y compris pour des spécialistes : c'est bien ce qui permet à l'ASIC d'interpréter le texte proposé. C'est surtout aussi une vulnérabilité pour le texte, dans la mesure où l'intelligibilité de la loi est un objectif à valeur constitutionnelle : une éventuelle censure du L 246-1 proposé mènerait sans doute à la suppression de la totalité de l'article 13 »*.

La méthode choisie par la majorité ne pose-t-elle pas tout de même certains problèmes, notamment en raison de la précipitation avec laquelle ce texte est voté, et du manque de débat ?

Si, bien sûr. C'est d'ailleurs, au-delà des attendus de notre avis, ce que nous avons souligné dans notre décision de nous saisir de cette grande question des libertés et des droits à l'ère numérique : il faut, sur des sujets aussi graves et protéiformes que ceux-là, prendre le temps d'en débattre, de se concerter avec toutes les parties prenantes (les services, les entreprises, la société civile, etc.).

Mais également, on ne peut traiter toutes ces questions segmentées dans différents projets ou propositions de loi au fur et à mesure qu'elles passent au parlement ! Le Conseil national du numérique en est à sa troisième saisine (dont deux auto-saisines) sur des sujets touchant aux libertés numériques. En l'occurrence, le débat actuel dépasse la seule loi de programmation militaire.

Or, nous sommes à un point de bascule absolument majeur dans les faits (l'attirail pour basculer dans une société de surveillance totale est potentiellement là) et dans les consciences (la défiance numérique commence à poindre).

Dans les faits, l'explosion des moyens technologiques d'observation et de contrôle dans une société totalement numérisée, et l'effondrement de leurs coûts, changent totalement la donne. Même Staline dans ses rêves les plus fous ne disposait pas des moyens matériels d'espionner les courriers postaux de 200 millions de citoyens soviétiques. La NSA, elle, le peut potentiellement sur plus d'un milliard d'individus ; mais pas seule : en utilisant l'accumulation incroyable de données de masse (Big Data) que nous tous laissons dans ces grandes plateformes, au quotidien. Et dont nous ne pouvons plus nous passer car elles sont hyper-innovantes et nous rendent des services qui ont changé nos vies ! Mais les faits sont là : potentiellement, nous pouvons basculer dans une société de surveillance totale où elle devient la règle, et non plus l'exception. C'est une situation inédite dans l'histoire de l'humanité. Ça mérite un vrai débat, non ? Et pas qu'en France…

Dans les consciences, l'affaire Snowden constitue une déflagration immense dans le champ numérique dont on n'a pas fini de mesurer l'impact : le risque de défiance du grand public est grand. Il progresse. Depuis, on note l'explosion des usages des moteurs de recherche qui ne vous traquent pas, des logiciels d'anonymisation de votre navigation de type TOR, ou même des applications de cryptage de vos mails. Certains analystes voient même, récemment, dans le tassement du commerce au ligne, un premier signe manifeste de cette défiance !

N'y a-t-il pas justement, en pleine affaire Snowden, un paradoxe à renforcer aujourd'hui notre propre dispositif de surveillance ?

Vous avez raison, on ne peut se contenter de cela. Il faut impérativement endiguer ce mouvement de défiance et rétablir la confiance du public vis-à-vis d'une société et d'une économie en voie de digitalisation totale. Pour cela, il faut se concerter, prendre le temps de débattre, et intégrer toutes ces dimensions dans une grande loi sur les libertés numériques. En 1978, la France a été pionnière, après le scandale du fichier SAFARI (le fameux fichier des honnêtes gens) dénoncé par Philippe Lemoine, notre premier lanceur d'alerte, et fut le premier pays à se

doter d'une loi protectrice de nos droits à l'heure de l'informatique émergente. Il faudra l'adapter. C'est pour cela que le CNNum lance une concertation qui vise à nourrir cette future grande loi que Fleur Pellerin a annoncée pour 2014, ce dont nous nous réjouissons.

Au niveau européen et international, il faut que la France reprenne la tête de ce mouvement à l'heure du tout numérique. Il nous faut reprendre la directive européenne sur ce sujet, qui s'est embourbée. Mais il est nécessaire également de ne pas s'en contenter et de porter un traité international pour servir de cadre à ces nouveaux usages et limiter ces dérives. La vision purement contractuelle des Américains (qui règlent l'essentiel de ces rapports par des CGU – conditions générales d'utilisation) n'est pas celle des Européens qui croient davantage au droit positif qui protège les individus. Que ce soit dans nos rapports aux données personnelles ou dans l'exercice de ces droits, les Européens ont une culture politique différente, liée pour beaucoup à notre histoire. À nous de les défendre. Le Brésil, l'Allemagne ont fait des propositions en ce sens.

Certains, au sein de la majorité, accusent des entreprises s'opposant à ce texte de vouloir *« se refaire une virginité »* alors que ce sont *« les majors de l'internet qui font commerce de milliards de données et qui coopèrent avec la NSA »*. Y a-t-il réellement une hypocrisie ou un double jeu de la part de certains acteurs ?

Je ne suis pas paranoïaque : je ne crois nullement à la collusion préméditée de ces plateformes avec les services de renseignements, même si les "telcos et les services" ont souvent convolé… Je pense que les majors de l'internet sont extrêmement embarrassées : j'ai des amis ingénieurs chez Google qui me font part de leur malaise et qui pensent que ces usages vont à l'encontre de leur éthique, de leur vision de ce qu'est internet depuis son origine (très libertaire, très californien), et même menacent le projet d'entreprise de Google voulu par ses fondateurs. Regardez d'ailleurs les propositions que viennent de faire les grandes plateformes américaines pour réformer les lois sur le renseignement US : elles savent qu'elles jouent gros et elles ont raison.

En revanche, je pense qu'il ne faut pas instrumentaliser le débat sur la LPM pour se détourner un peu facilement des graves questions posées par l'affaire Snowden ! Ce serait un comble : la DGSE en sait moins sur chacun de nous, citoyens français, que Facebook ou Google, et ça n'est pas l'exploitation de Deezer ou de Dailymotion par la DCRI qui peut atteindre les niveaux de scandale de l'affaire PRISM ! Mais on voit bien qu'il est difficile d'avoir un débat équilibré et serein à chaud. Encore plus à l'heure de Twitter ! D'où notre appel à une concertation large, et qui prenne le temps.

Mais il faut aussi revenir à l'origine de tout cela : l'incroyable durcissement des législations sécuritaires post 11-Septembre, initiées par George W. Bush, dont le Patriot Act fut probablement la quintessence. David Cameron a été l'un des rares dirigeants occidentaux à poser la question de la nécessité de revisiter ces lois et dispositifs. Ce durcissement, conjugué au Big Data, et à la numérisation des usages de nos vies quotidiennes, est devenu explosif. Il est temps d'en discuter et de réagir. Car ne l'oublions pas : jusque-là, la révolution numérique a été un formidable levier d'*empowerment* pour les individus et les sociétés. C'était d'ailleurs le projet politique des pères fondateurs de l'internet. Il ne faut pas dévier de ce fabuleux projet d'*empowerment* qui est en train de changer le monde.

Boite noire

Benoit Thieulin est également directeur de l'agence digitale La Netscouade. A ce titre, il a joué un rôle important dans la création de Mediapart, notamment sur l'aspect participatif. Sa société a réalisé le site et en a par la suite effectué plusieurs refontes.

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.

Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.